Security Architecture for Aeronautical Networks

Bob Stephens

Boeing Air Traffic Management
Tectura Corporation

robert.w.stephens2@boeing.com

Purpose of Security

- Protect systems and resources from unauthorised use
- Ensure the proper operation of those systems
- Application of security is:
  - Not arbitrary
  - Result of a properly conducted Threat/Vulnerability/Risk Analysis
    - Determine the security threats from which protection is required
    - Implement Security functions that collectively provide an appropriate set of countermeasures to those threats

Outline of Presentation

Security Mechanisms and Technologies

Reference Security Model

Security Policies

- A document that defines the sensitivity of the information being processed and the measures that are used to protect the information
- Security policies exist from a high-level down to a low-level of detail
- Security policies should be revised as needed

Aviation Security Requirements

- Air-Ground and Ground-Ground Communications
  - Air Traffic Control (ATC)
  - Airline Operational Communications (AOC)
  - Airline Administrative Communications (AAC)
  - Airline Passenger Communications (APC)
- Onboard Networks
  - Aircraft Control
  - Airline Information Services
  - Passenger Information and Entertainment Services

Network Security Mechanisms and Technologies

- Cryptographic network security
- Non-Cryptographic network security

- Communications level security
- Application level security

Cryptographic Security Definitions

- Authentication - The assurance to one entity that another entity is who he/she/it claims to be.
- Integrity - The assurance to an entity that data has not been altered (intentionally or unintentionally) between "there" and "here," or between "then" and "now."
- Confidentiality - The assurance to an entity that no one can read a particular piece of data except the receiver(s) explicitly intended.
- Nonrepudiation – The ability to ensure that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

Communications Security and Application Security

- Security can be deployed at different levels of the OSI reference model
- Communications security
  - Transparent to applications
  - Examples: IPsec, VPNs, packet filter firewalls
- Application security
  - Involves the application
  - Examples: SSL, proxy servers, ATN security

Cryptographic Security Mechanisms

- Examples:
  - IPsec – Network Layer 3
  - SSL/TLS – Transport Layer 4
  - ATN – Application Layer 7

Cryptographic Key Schemes

- Shared Secret
  - Each end of a conversation shares a common key that is secret to them
  - Key distribution is a challenge
- Public Key
  - Each end of a conversation owns a confidential private key and a corresponding public key
  - Public key distribution is through certificates

Classes of Cryptographic Mechanisms

- Data origin and integrity protection
- Bulk data encryption using symmetric encryption algorithms
- Public-key authentication and key exchange
- Public-key infrastructure mechanisms in order to provide users with the needed credentials

Data Origin Authentication and Integrity Protection

- Keyed, one-way hash function which takes as input a message of arbitrary length and key of fixed length, producing a hash value of fixed length (can be truncated)
- Symmetric key is shared between both parties
- A sequence number is present or appended to input to protect against reordering
- Recommended algorithm is HMAC-SHA-1-96 (Hashed Message Authentication Code, Secure Hash Algorithm, truncated to 96 bits)

Key Exchange

- A shared symmetric key can be securely developed between to parties using a Diffie-Hellman or Elliptic Curve Diffie-Hellman algorithm
- Key length should be at least 1024 bits or 160 bits for elliptic curve

Bulk Data Encryption

- Provide for confidentiality of exchanged data
- Symmetric key is shared between both parties
- Preferred choice for new implementations is the Advanced Encryption Standard (AES) with 128-bit or larger keys

Public-Key Algorithms for User Authentication

- Pre-shared keys or public keys
- Pre-shared keys is not scalable to support size of the air transport business; public keys are recommended
- ATN recommends the use of Elliptic Curve Cryptography due to stronger security with shorter key lengths (for air-ground transmission efficiency)

Notes

- All cryptography implementations should allow for the easy introduction of new algorithms in case one is broken –mathematically or increase in computation speed capabilities
- Systems that implement cryptography should negotiate to an agreed set of algorithms that provide the highest level of security achieved with an acceptable security level and performance

Internet Protocol Security - IPsec

- IPsec stands for Internet Protocol security. It is the Internet standard for network layer security. IPSec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices.

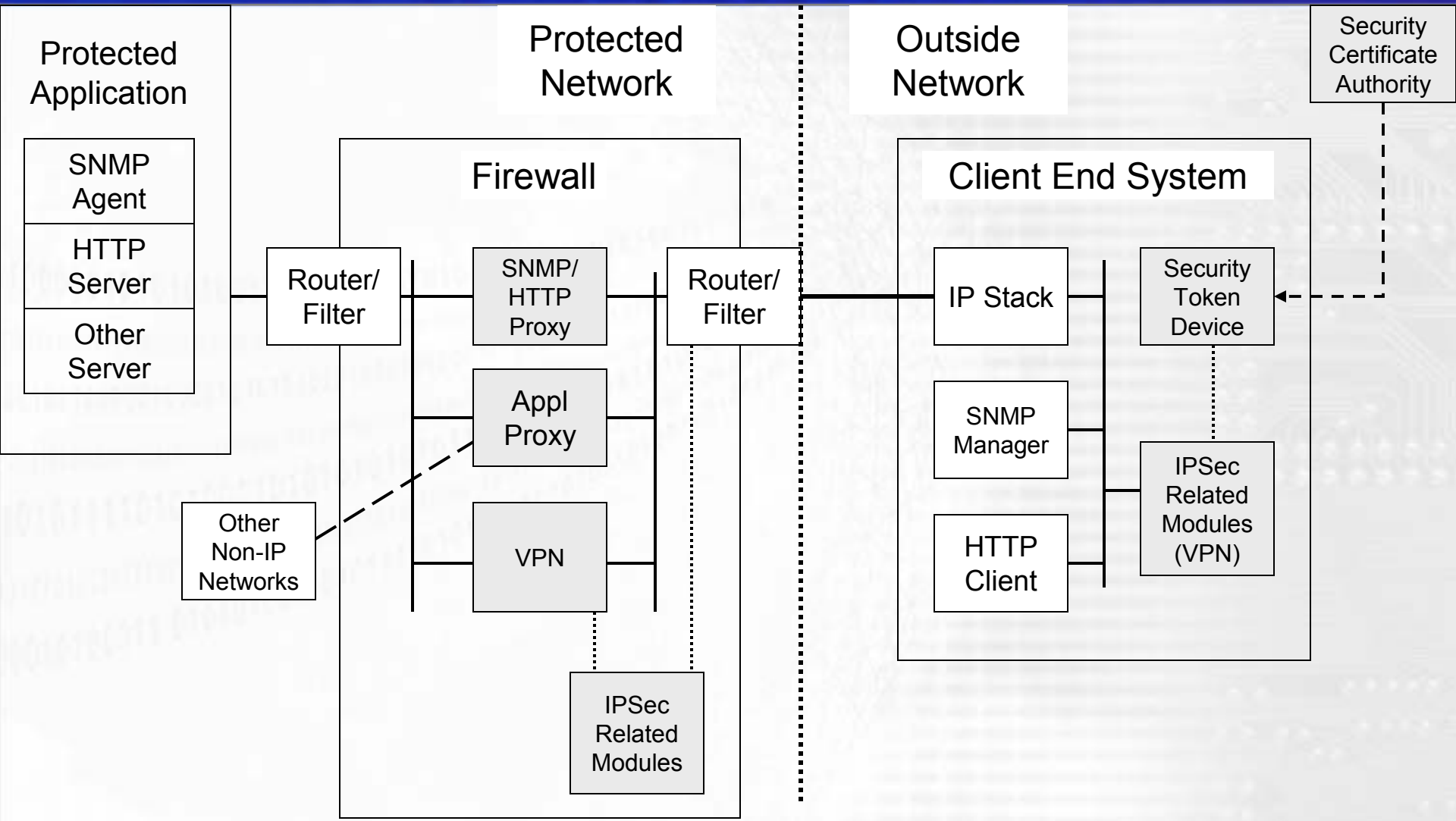
Non-Cryptographic Security Mechanisms

- Firewall controls the flow of traffic between two or more networks or traffic into a computer
- Defends against
  - Unauthorized access
  - IP address spoofing
  - Session hijacking
  - Rerouting of traffic
  - Denial of Service

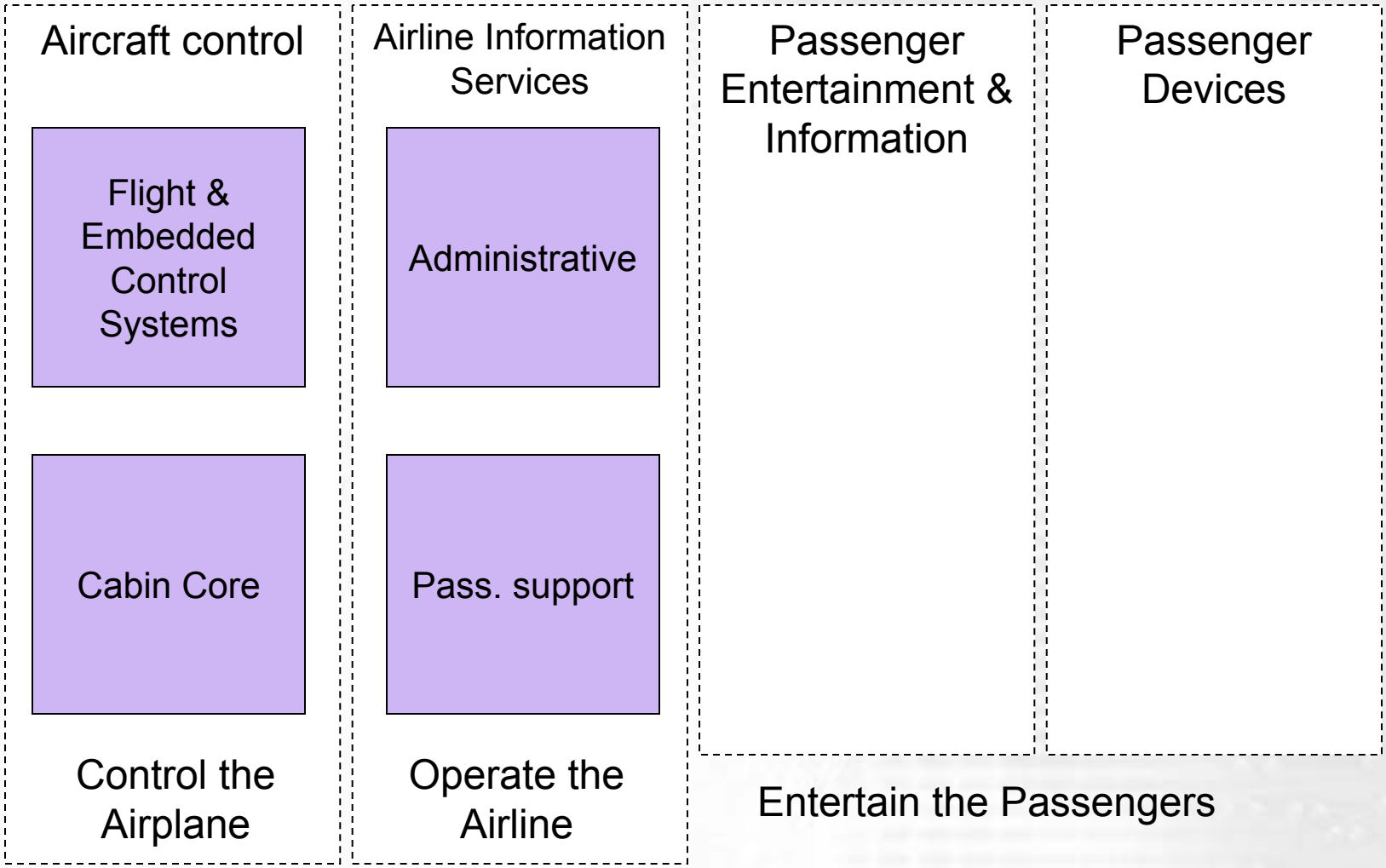
Non-Cryptographic Security Mechanisms

- Stateless packet filters
- Stateful packet filters
- Application level security proxies
- Circuit level gateways
- Intrusion Detection Systems

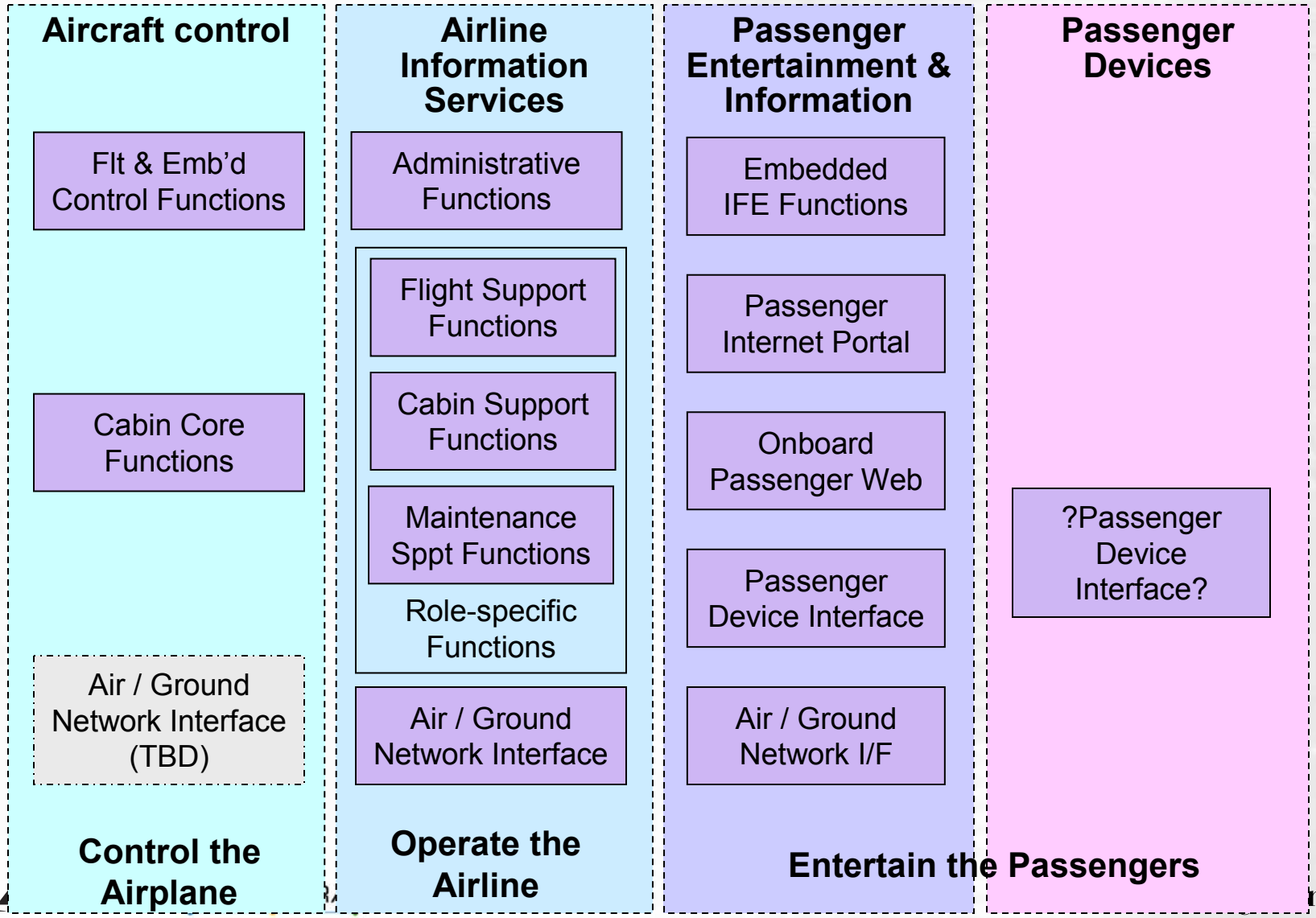
Reference Network Security Architecture



ARINC 664 Aircraft Data Networks - Domains

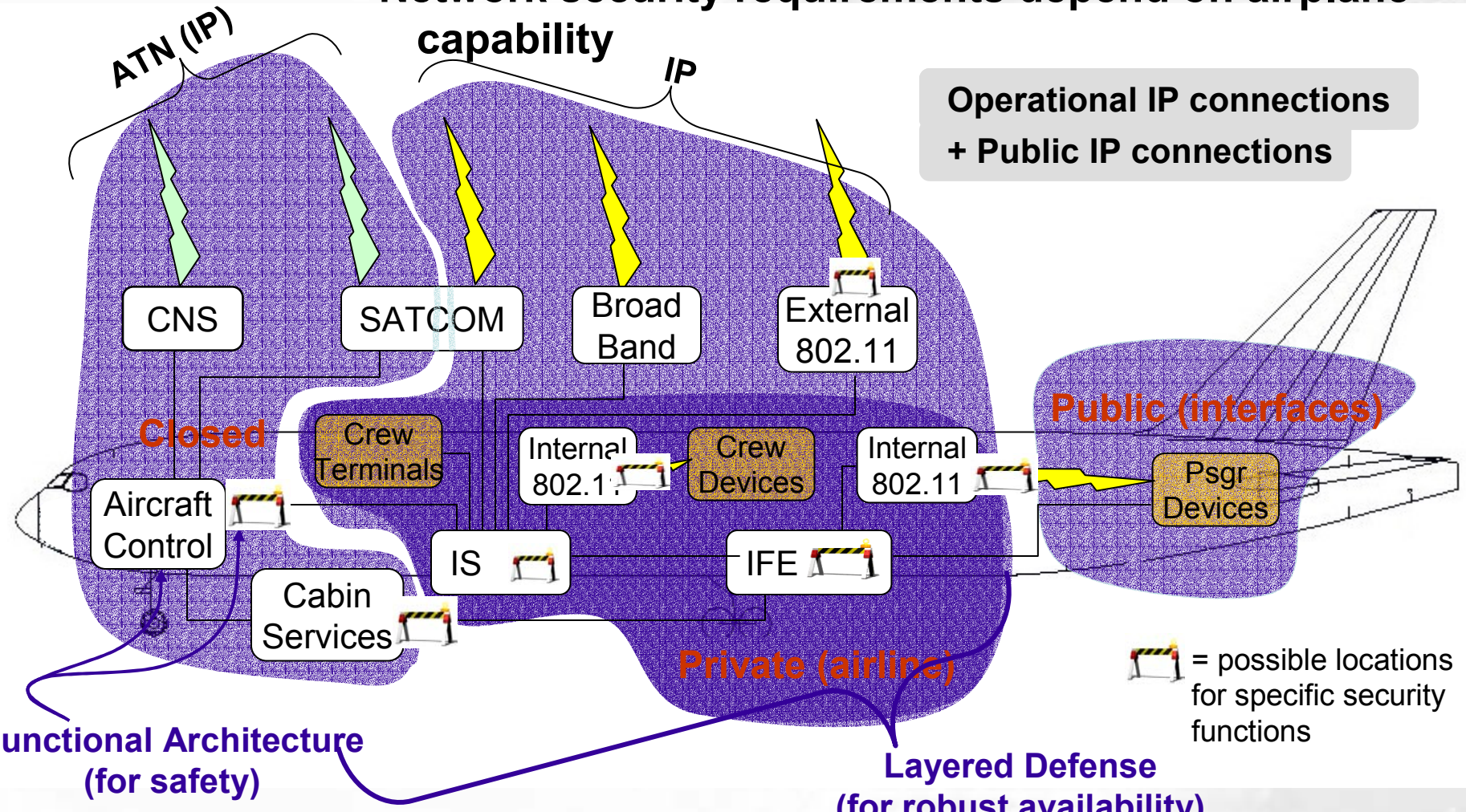


Aircraft Domain Breakout



Onboard Network Security

Network security requirements depend on airplane capability



Defense in Depth

- Mechanisms at multiple levels of the OSI reference model
  - Link layer
  - Network layer
  - Transport layer
  - Application layer
- Both cryptographic and non-cryptographic mechanisms

Summary

- **Security Mechanisms and Technologies**
  - Communications level security
  - Application level security
  - Non-cryptographic mechanisms
  - Cryptographic mechanisms
    - Key Distribution – Shared Secret or Public Key
- **Reference Security Model**
  - Ground and aircraft use
  - Onboard aircraft domains